U.S. Department of State
Privacy Impact Assessment Summary

TITLE: Online Passport Status Service (OPPS)
May 22, 2007

I. Describe the information to be collected (e.g., nature and source). Be sure to include any information in an identifiable form, e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc).

The system requests identifying information from the applicant, retrieves the latest status of the passport application (i.e. received, working, approved, mailed), and returns this information to the user. To identify him/herself, the applicant is required to submit his/her surname, date of birth, and the last four digits of his/her social security number.

II. Why is the information being collected (e.g., to determine eligibility)?

To allow the public (via OPSS) to indirectly access their passport application status information from the central repository.

III. How will the information be used (e.g., to verify existing data)?

To allow an individual to retrieve the latest status of the passport application (i.e. received, working, approved, mailed).

IV. Will you share the information with others (e.g., another agency for a programmatic purpose)? If yes, list the entities.

No, this is just a tracking device.

V. Describe what opportunities individuals have been given to decline to provide information or to consent to particular use of the information (e.g., whether individual may withhold permission for a particular use).

The information has already been submitted by the passport applicant, thus they have no opportunity to decline to provide it.

VI. How will the information be secured (e.g., administrative and technological controls)?

The OPSS system is deployed on a web and database server residing inside of OpenNet and on a web and database server residing inside of IRM's publicly accessible DMZ. Only a single firewall port is required to be opened to allow the database replication to occur from the OpenNet database to the DMZ database. No other connections are required between the OpenNet and DMZ servers. Connection between the OpenNet and DMZ database servers is via Oracle Database Replication using a secure socket layer (SSL) with 128-bit data encryption. The source of all data contained within the OPSS databases is the database on OpenNet, and the original source of this data is the TDIS repository server, which is outside the scope of the OPSS system boundary. There is no requirement to store web user data or user personal data within the OPSS system. Since there is no data processing at the DMZ, there are no special security considerations for OPSS outside of the normal security concerns of any public-facing Internet accessible DoS web site.

VII. How will the data be retrieved (e.g., will it be retrieved by a personal identifier such as name, social security number, address, telephone number or some other identifier that is unique to an individual)?

The system will request identifying information from the applicant, retrieve the latest status of the passport application (i.e. received, working, approved, mailed) and return this information to the user. To identify him/herself, the applicant will be required to submit his/her surname, date of birth, and the last four digits of his/her social security number.